BlackRidge Technology

Transport Access Control (TAC) Gateways

R4.2.1 CLI-Based Installation Shortcut Guide for Layer3

Part No. SCGL3-CLI-00042-01-04
Revision 1.4, March 2019

BlackRidge TECHNOLOGY

Contents

Document Part Number: Part No. SCGL3-CLI-00042-01-04

Preface

From the Publisher

The *Technical Publications* group at BlackRidge Technology, Inc. is committed to providing you timely, accurate technical product documentation that is both instructive and easy-to-use.

To that end, we apply our internal resources to design and develop comprehensive technical content to support the installation, configuration and deployment of our product line, and to test the quality and utility of each product document before releasing to our customers.

Unfortunately, no internal process based on people is perfect. There may be occasions when an error gets by our internal quality assurance process and appears in a released document. We apologize in advance if this document has such an error(s).

We would, however, appreciate your help in notifying us in the event you discover any errors—grammatical or otherwise—by identifying the error(s) and its location in the document, and sending it in an e-mail to: techpubs@blackridge.us.

We also welcome any recommendations you might have that would enhance or improve the overall utility of our technical product documentation suite. Your contributions can make a difference in our efforts to reach and maintain the goal of error-free, easy-to-use technical product documentation.

Thank you in advance…

—Technical Publications, BlackRidge Technology, Inc.

About This Guide

This *Installation Shortcut Guide* is an optional document for TAC administrators with previous knowledge and experience with installing BlackRidge TAC Gateway(s).

Warning: For security and protection purposes, each BlackRidge TAC Gateway must have a valid certificate signed by BlackRidge Technology, before it can operate in production. Therefore, it is required that the procedures outlined in the BlackRidge Certificate Signing Request (CSR) section of the platform-specific *R4.2.1 Installation and Configuration Guide,* be completed before performing any task outlined in this guide.

The procedures outlined in this command line interface (CLI)-based *Installation Shortcut Guide* provide guidance in achieving basic Layer3 configurations of the BlackRidge TAC Gateways, with minimal effort and time. It is designed to enable the experienced TAC administrator to successfully leverage the cloaking capabilities of the BlackRidge TAC Gateways via the CLI.

It makes no attempt to cover all the administrative aspects of the command line interface (CLI) for configuring the product. Instead, a simple configuration is used as the basis for introducing a subset of the commands supported by the product.

This *CLI-based Shortcut Guide* provides the minimum set of commands required to achieve the following:

- Configuring the *TAC Identity Inserter* Gateway to trust a IPv4 network endpoint
- Assigning that trusted IPv4 endpoint, the ***Trusted Host,*** to a ***Group***
- Configuring the Publisher-Subscriber Service on the *Identity Inserter Gateway*
- Configuring the NAT and route functions to support Layer3
- Configuring the TAC *Identity Resolver* Gateway to protect a IPv4 network endpoint
- Creating a rule to govern the communications between networks and endpoints connected by BlackRidge TAC Gateways
- Configuring the Publisher-Subscriber Service on the *Identity Resolver Gateway*
- Employing *Distributed Identities* to configure unidirectional authentication for all network communications between two IPv4 endpoints (e.g., ***Trusted Host*** and ***Protected Resource***) connected through two BlackRidge TAC Gateways
- Enabling Transport Access Control (TAC) on a network endpoint defined as a ***Protected Resource,*** effectively removing it from unauthorized access, awareness and reconnaissance.

For more instructive text and guidance for installing BlackRidge TAC Gateways, refer to the platform-specific *R4.2.1 Installation and Configuration Guide*.

For descriptions of the CLI commands, refer to the *BlackRidge Release 4.2.1 Command Reference*.

Who Should Use This Guide

This guide is intended for experienced IT and networking professionals who are responsible for the basic configuration of the various BlackRidge TAC Gateways comprising the BlackRidge product line.

It is designed for those who have previous working knowledge and experience with deploying, installing and configuring BlackRidge TAC Gateway appliances. As such, it contains minimal guidance for the procedures outlined within this document.

How This Guide is Organized

Section I provides the sample Layer3 network topology highlighting the minimum set of commands required to configure the gateway to support a *Distributed Identity*-based ***Protected Resource.*** This is to be used by those who have previous knowledge and experience with configuring previous versions of the BlackRidge TAC Gateway appliances.

Section II provides the sample Layer3 network topology highlighting the minimum set of commands required to configure the gateway to support a *Distributed Identity*-based ***Trusted Host*** with limited instructive text. This is to be used by those who have previous knowledge and experience with configuring previous versions of the BlackRidge TAC Gateway appliances.

Typographical Conventions

This document uses the following typographic conventions to help you locate and identify information:

Italic text

Identifies new terms, emphasis, and book titles

Bold text

Identifies button names and other items that you can click or touch in the graphical user interface or press on a computer keyboard

`Courier New`

Identifies commands, command syntax, command arguments and system prompts

`Bold Courier New`

Identifies command strings being executed by the system via the CLI.

Note: Notes provide extra information about a topic that is good to know but not essential to the process.

Caution: Cautions draw your attention to actions that could compromise the security of your system or result in the loss of data.

SECTION I—Configuring Layer3 Distributed Identity-Based Protected Resources

Topology for Layer3-Enabled IPv4 Network Endpoints with Distributed Identities

The objective of this of this guide is to enable the administrator to achieve the following configuration:

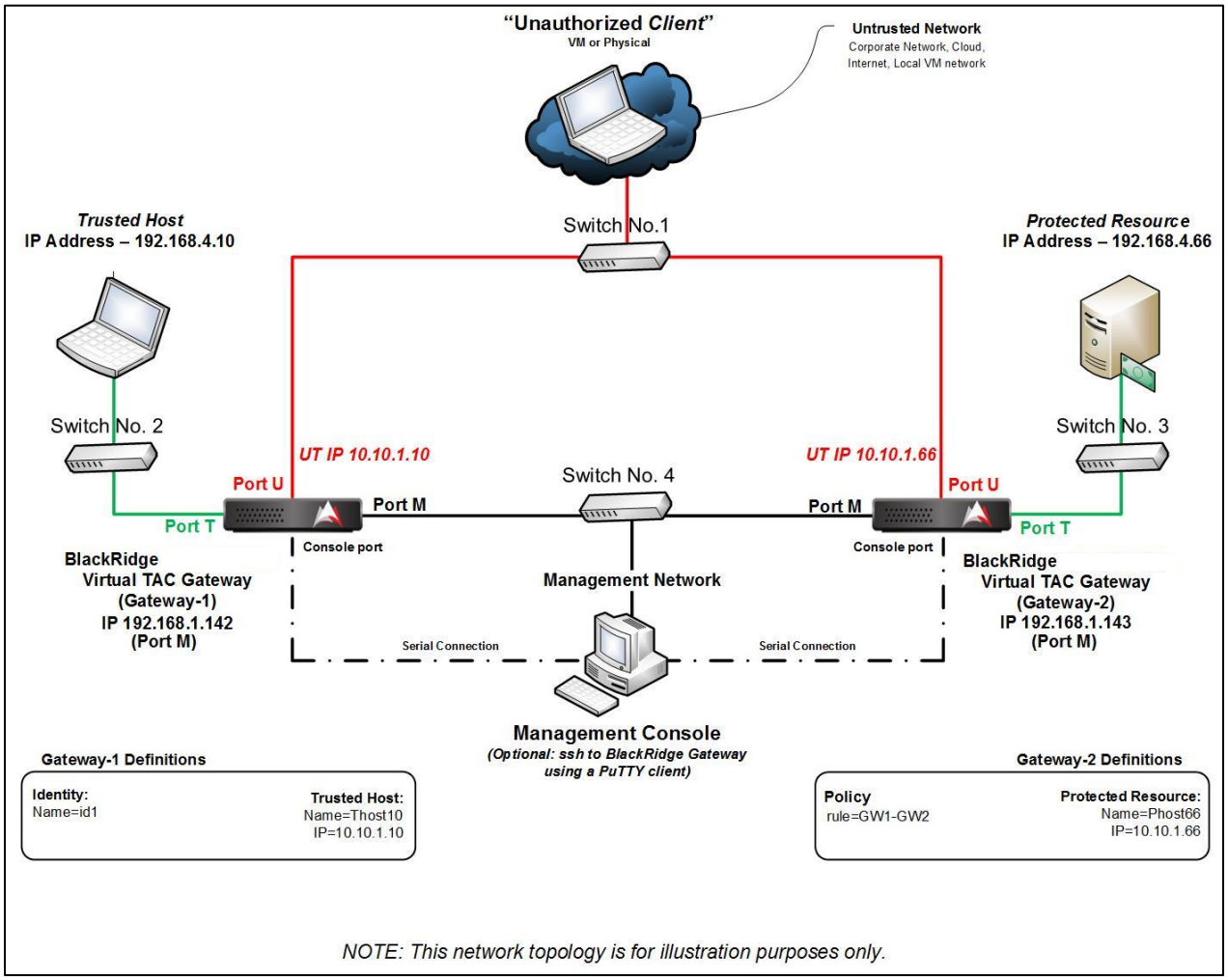

Figure 1.1 – Unidirectional Authentication of Two Network Endpoints Using Layer3

The configuration comprises the following:

- Two BlackRidge TAC Gateways, **Gateway-1** performing *Network Address Translation* (NAT) and *Identity Insertion* and **Gateway-2** performing *Network Address Translation*, *Identity Resolution and policy enforcement*

- One ***Trusted Host,*** node name *Thost10* with the private, ***Trusted IP address*** *192.168.4.10 – mapped to a public,* ***Untrusted IP address*** *of 10.10.1.10* initiates:
    - TCP/IP connection requests to the ***Protected Resource***

- One **Protected Resource**, node name Phost66 with a private, ***Trusted IP address*** 192.168.4.66 – mapped to a public, ***Untrusted IP address*** of 10.10.1.66 accepts:
    - TCP/IP connection requests from the ***Trusted Host***

- One ***Unauthorized Client*** that can be used as an attack system to verify proper configuration of the BlackRidge TAC Gateways—it should not be able to access the ***Protected Resource***.

Layer3 Configuration Definitions for Gateway-2

This page contains the definitions and commands to configure Layer3 on the *Identity Resolver Gateway*, Gateway-2, to support one IPv4 network endpoint defined as a ***Protected Resource*** and to configure ***Distributed Identities.***

This configuration enables this network endpoint to participate in unidirectional authentication with another network endpoint that is defined as a ***Trusted Host***.

Caveat: The following definitions and values are strictly used for illustration purposes only. Use definitions and values that are appropriate for your unique security requirements and local environment.

GATEWAY-2 NAT DEFINITIONS	
OBJECT	VALUE
tr_ip	192.168.4.66
Prefix	24
tr_vlanid	0
ut_ip	10.10.1.66
Prefix	24
ut_vlanid	0
ps	

Table 1.1 – Definitions Used to Configure Layer3 Connectivity on Gateway-2

GATEWAY-2 ROUTE DEFINITIONS	
OBJECT	VALUE
Trusted_flag	Y
ip	192.168.4.1
prefix	24
vlanid	0

Table 1.2 – Definitions Used to Configure Layer3 Routes on Gateway-2

GATEWAY-2 ROUTE DEFINITIONS	
OBJECT	VALUE
Trusted_flag	N
ip	10.10.1.1
prefix	24
vlanid	0

Table 1.3 – Definitions Used to Configure Layer3 Routes on Gateway-2

Distributed Identity Definitions for Gateway-2

This page contains the definitions and commands to configure an *Identity* on the *Identity Resolver Gateway*, Gateway-2, to support one IPv4 network endpoint defined as a ***Protected Resource*** and to configure ***Distributed Identities.***

This configuration enables this network endpoint to participate in unidirectional authentication with another network endpoint that is defined as a ***Trusted Host***.

Caveat: The following definitions and values are strictly used for illustration purposes only. Use values that are appropriate for your unique security requirements and local environment.

GATEWAY-2 PROTECTED RESOURCE DEFINITIONS	
OBJECT	VALUE
Protected Resource	Phost66
IP Address	10.10.1.66
Prefix	32
Rule	GW1-GW2
Group	group1

Table 1.4 – Definitions Used to Create a Protected Resource in Layer3 Mode

GATEWAY-2 SUBSCRIBER DEFINITIONS	
OBJECT	VALUE
Groups	group1
Token Gen Algorithm	HMAC-SHA-256
Publisher IP	192.168.1.142
Timeout (seconds)	3601

Table 1.5 – Definitions Used to Configure Gateway-2 as a Subscriber Gateway in Layer3 Mode

Commands for creating a Protected Resource(s) as a Distributed Identity with Access Policy Rule(s) for Layer3 Mode

DEFINING 192.168.4.66 AS A PROTECTED RESOURCE
/layer3/nat/add tr_ip=192.168.4.66/24 tr_vlanid=0 ut_ip=10.10.1.66/24 ut_vlanid=0 /layer3/route/add trusted_flag=y ip=192.168.4.1/24 vlanid=0 /layer3/route/add trusted_flag=n ip=10.10.1.1/24 vlanid=0 /layer3/enable /policy/rule/resource/add name=Phost66 ip=10.10.1.66/32 /policy/rule/add name=GW1-GW2 action=forward resource=Phost66 identity_group=group1 enable=yes trust_level=5 /identity/distributed/cfg groups=group1 token-gen- algorithm=HMAC-SHA-256 publisher=192.168.1.142 timeout=3601 /identity/distributed/enable /identity/distributed/subscriber operation=start /identity/distributed/cfg /identity/show save

Table 1.6 – Commands for creating a Protected Resource(s), Policy Rule(s) as a Distributed Identity

COMMANDS TO REMOVE 192.168.4.66 AS A PROTECTED RESOURCE
/policy/rule/del name=GW1-GW2 /policy/rule/resource/del name=Phost66 save

Table 1.7 – Commands for removing an Identity-based Policy

VERIFICATION COMMANDS
/etc/hostname/show /etc/hosts/show /identity/show /identity/distributed/cfg /policy/rule/show /policy/rule/resource/show /policy/rule/resource/list/show /context/show

Table 1.8 – Commands for verifying the removal of a Protected Resource and Policy

SECTION II—Configuring Layer3 Distributed Identity-Based Trusted Hosts

Topology for Layer3-Enabled IPv4 Network Endpoints with Distributed Identities

The objective of this of this guide is to enable the administrator to achieve the following configuration:

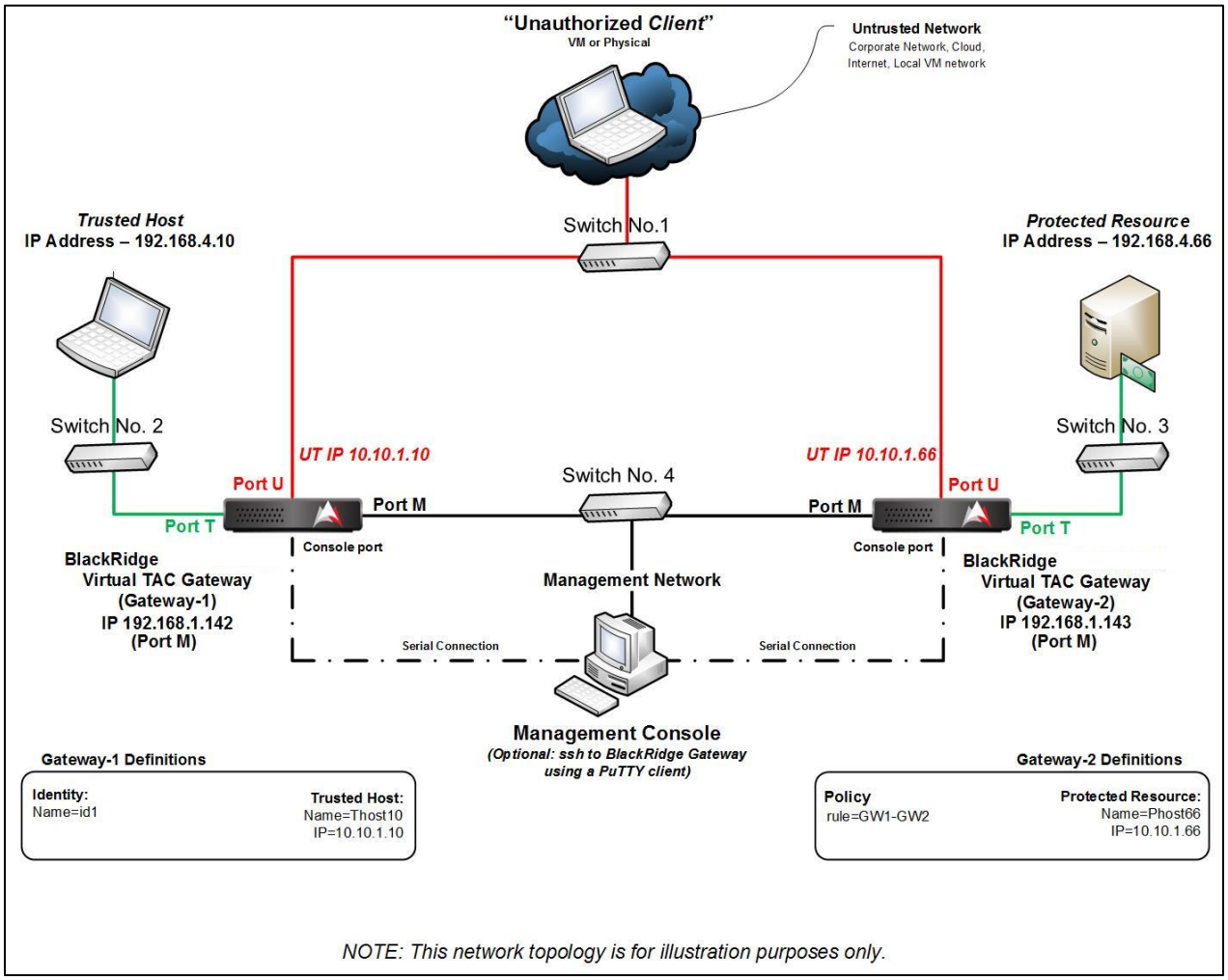

Figure 2.1 – Unidirectional Authentication of Two Network Endpoints Using Layer3

The configuration comprises the following:

- Two BlackRidge TAC Gateways, **Gateway-1** performing *Network Address Translation* (NAT) and *Identity Insertion* and **Gateway-2** performing *Network Address Translation*, *Identity Resolution and policy enforcement*

- One ***Trusted Host,*** node name *Thost10* with the private, ***Trusted IP address*** *192.168.4.10 – mapped to a public,* ***Untrusted IP address*** *of 10.10.1.10* initiates:
    - TCP/IP connection requests to the ***Protected Resource***

- One **Protected Resource**, node name Phost66 with a private, ***Trusted IP address*** 192.168.4.66– mapped to a public, ***Untrusted IP address*** of 10.10.1.66 accepts:
    - TCP/IP connection requests from the ***Trusted Host***

- One ***Unauthorized Client*** that can be used as an attack system to verify proper configuration of the BlackRidge TAC Gateways—it should not be able to access the ***Protected Resource***.

Layer3 Configuration Definitions for Gateway-1

This page contains the definitions and commands to configure Layer3 on the *Identity Inserter Gateway*, Gateway-1, to support one IPv4 network endpoint defined as a ***Trusted Host***.

This configuration enables this network endpoint to participate in unidirectional authentication with another network endpoint that is defined as a ***Protected Resource***.

GATEWAY-1 NAT DEFINITIONS	
OBJECT	VALUE
tr_ip	192.168.4.10
Prefix	24
tr_vlanid	0
ut_ip	10.10.1.10
Prefix	24
ut_vlanid	0
ps	

Table 2.1 – Definitions Used to Configure Layer3 connectivity on Gateway-1

GATEWAY-1 ROUTE DEFINITIONS	
OBJECT	VALUE
Trusted_flag	Y
ip	192.168.4.1
prefix	24
vlanid	0

Table 2.2 – Definitions Used to Configure Layer3 Routes on Gateway-1

Distributed Identities Definitions for Gateway-1

This page contains the definitions and commands to configure an *Identity* on the *Identity Inserter Gateway*, Gateway-1, to support one IPv4 network endpoint defined as a ***Trusted Host***. The section includes steps to configure the ***Distributed Identities***. Gateway-1 will be configured as a ***Publisher*** gateway.

This configuration enables this network endpoint to participate in unidirectional authentication with another network endpoint that is defined as a ***Protected Resource***.

GATEWAY-1 TRUSTED HOST DEFINITIONS	
OBJECT	VALUE
Identity	id1
Group	group1
Enable	yes
Trust Level	5
IP Address	10.10.1.10
Prefix	32
MAC	
Tagging	seq
Comment	

Table 2.2 – Definitions Used to Create an Identity in Layer3 Mode

GATEWAY-1 PUBLISHER DEFINITIONS	
OBJECT	VALUE
Groups	group1
Token Gen Algorithm	HMAC-SHA-256
Publisher IP	192.168.1.142
Timeout (seconds)	3601

Table 2.3 – Definitions Used to Configure Gateway-1 as a Publisher Gateway in Layer3 Mode

Commands for creating a Trusted Host(s) as a Distributed Identity for Layer3 Mode

CONFIGURING 192.168.4.10 AS A TRUSTED HOST
/layer3/nat/add tr_ip=192.168.4.10/24 tr_vlanid=0 ut_ip=10.10.1.10/24 ut_vlanid=0 /layer3/route/add trusted_flag=y ip=192.168.4.1/24 vlanid=0 /layer3/route/add trusted_flag=n ip=10.10.1.1/24 vlanid=0 /layer3/enable /identity/add name=id1 group=group1 enable=yes trust_level=5 ip=10.10.1.10/32 tagging=seq /identity/distributed/cfg groups=group1 token-gen- algorithm=HMAC-SHA-256 publisher=192.168.1.142 timeout=3601 /identity/distributed/enable /identity/distributed/cfg /identity/show save

Table 2.4 – Commands for Creating an Identity

COMMANDS TO REMOVE 192.168.4.10 AS A TRUSTED HOST
/identity/del id1 save

Table 2.5 – Commands for removing an Identity

VERIFICATION COMMANDS
/etc/hostname/show /etc/hosts/show /identity/show /identity/distributed/cfg /policy/rule/show /policy/rule/resource/show /policy/rule/resource/list/show /context/show

Table 2.6 – Commands for verifying the removal of an Identity Trusted Host