

How drut. helps you monitor your firewalls

December 2023

Robotics GRC



drut.
speed on the wire



Ever wondered how they manage that?

What vulnerabilities do hackers use to get around seemingly watertight network security defences?

- Statistics prove that hackers mostly do this by getting around firewalls

But it's not all doom and gloom

We have the most comprehensive and detailed ways to continuously increase the level risk monitoring risks on your firewalls

**Ways a Firewall
can get
Breached**

Incorrectly configured rules

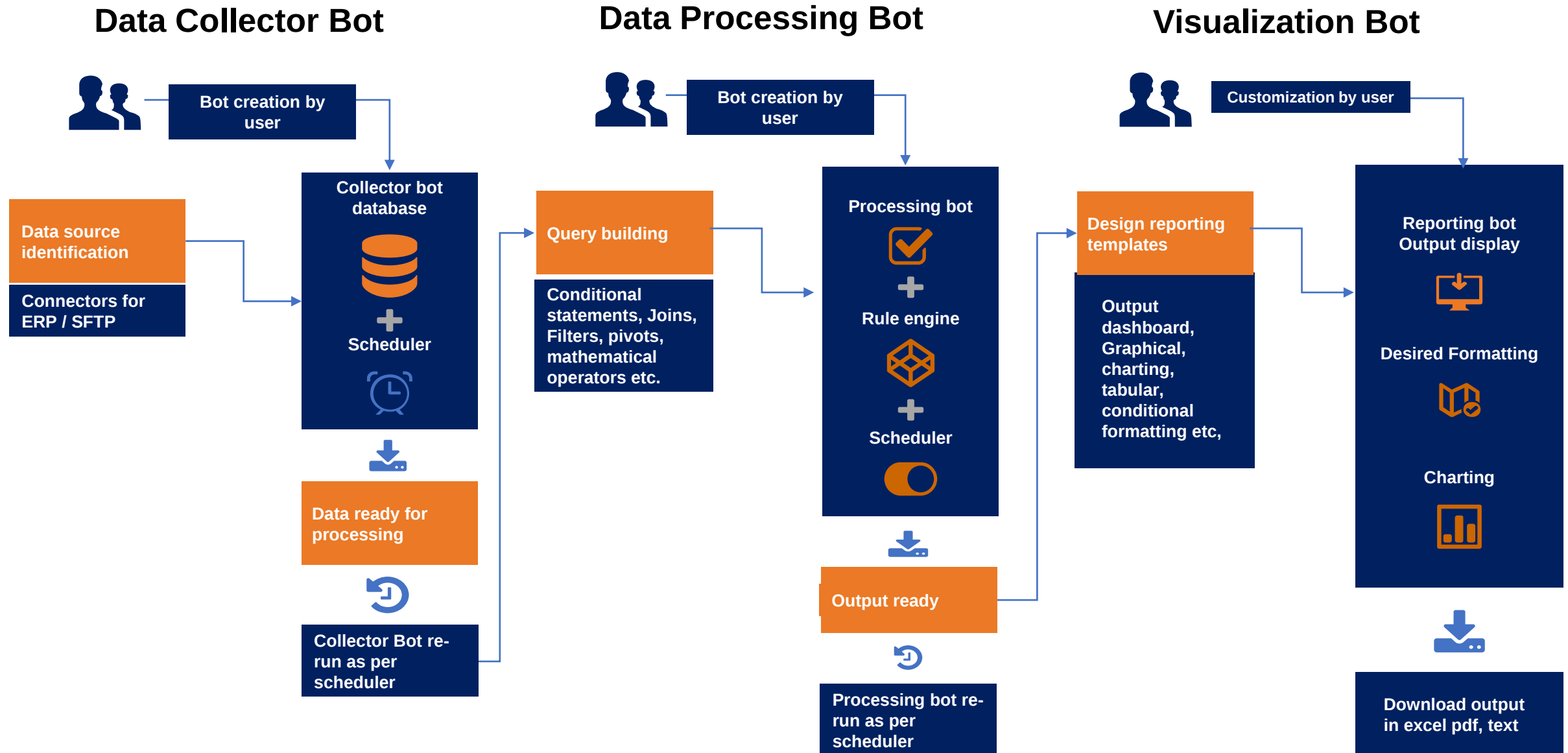
Unsecured remote access

Malware infection

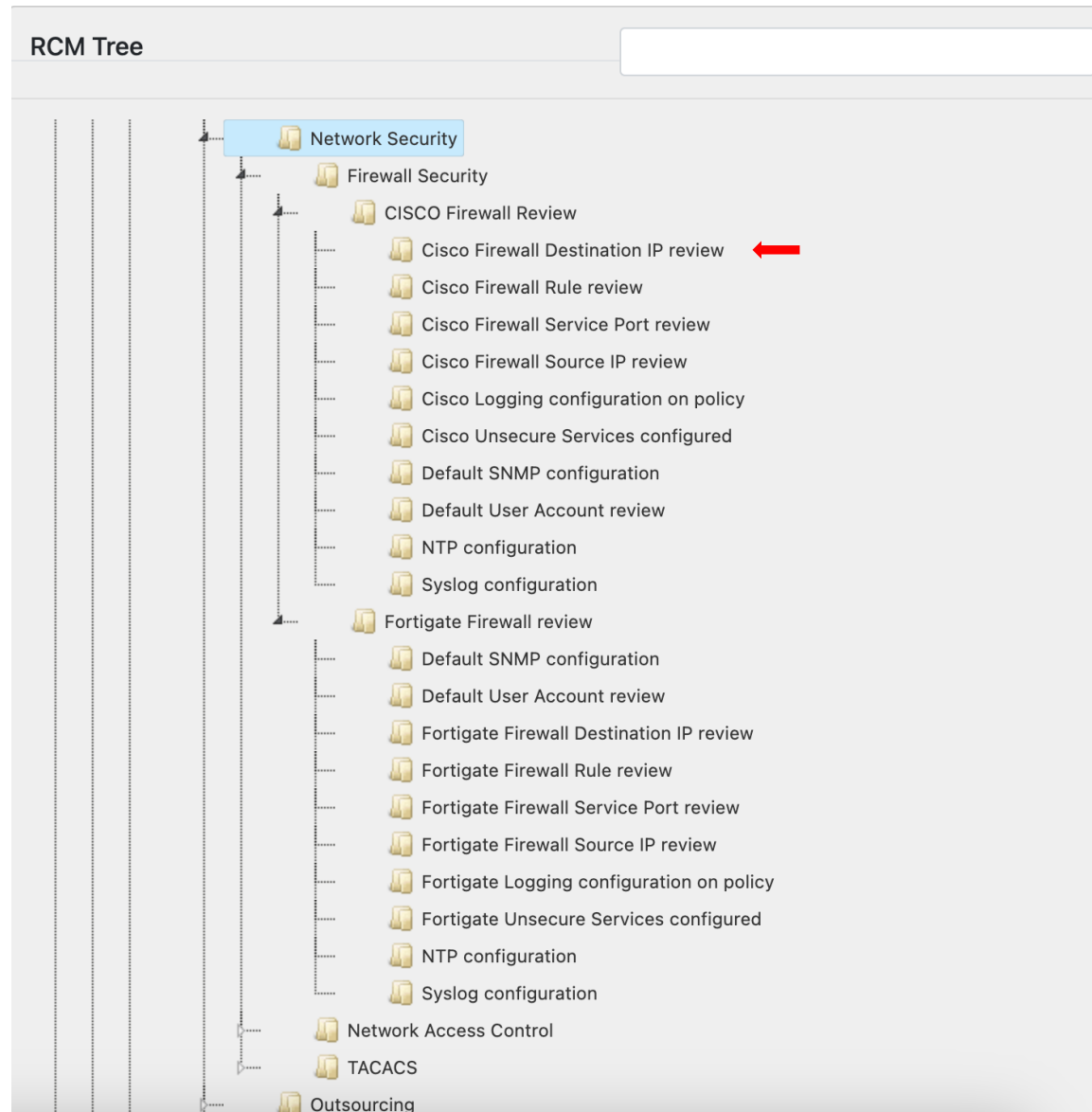
Weak passwords

Outdated software

how drut will help in Automation of Firewall Review?



Find your control in drut.'s RCM – Risk Control Matrix



Incorrectly Configured Rules - 1.run the bot



drut.

Grid

Folder

Tree

Bot

Shield

Document

Checkmark

Help

Export

RCM

Search For

Switch to ReportBI ☐

ANB / ANB Group / Kohinoor Bank / Technology / Network Security / Firewall Security / CISCO Firewall Review / Cisco Firewall Destination IP review

Show entries

Search:

RCM Tree

↕	Sub Process ↕	Activity ↕	Risk ↕	Severity ↕	Control ↕	Automatable ↕	CheckPoint ↕	Update ↕	Robo ↕
	Cisco Firewall Destination IP review	To ensure that firewall destination IP addresses are configured correctly	Rules which allow or accept any or all destination might lead to unauthorized and unrequired access to information systems	High	Rules with any or all destination should be denied or rejected or specified IP address or network should be configured in destination address to allow specific required access	Yes	Verify that Firewall rules is not configure with ANY or ALL Destination IP Address	Edit Activity Edit Risk	Add Collector Add Analysis

Bot Name	Condition Name	Bot Type	Bot For	Schedule Type	Last Run Time	Next Run Time	Bot Status	Results	Edit	Delete
Destination IP check	Rules with Any or All destination should be denied or rejected or specified IP address or network should be configured in destination address to allow specific required access	Analysis	Database	RunOnce	02/08/2023 17:51:17 PM	02/08/2023 17:44:00 PM	Finished	View Exceptions View ReportBI Add Risk Parameter Add Summary	Edit	

Showing 1 to 1 of 1 entries

Previous 1 Next

Download Full RCM

☒ Company ☐ Department ☐ Sub Department

2. find the exceptions

drut.

Grid

Layers

Network

Robot

Shield

Document

File

?

→

View Report

Search For

Switch to ReportBI

Activity : To ensure that firewall destination IP addresses are configured correctly

Annexure : Number of instances where Firewall rules is configure with ANY or ALL Destination IP Address

Base Data132090

Total Number of Rows in Base Data

Exceptions273

Number of Exceptions in Report

Deviation0%

Deviation between Total Rows and Exceptions

0406080100

0% Low Risk

Download

Bar Chart

Line Chart

Table

Summary

Preview Result

Cards & Charts

Pivot Result

Base Files

Columns: Hide

Sorting: Off

View Data: Lazy Loading

Search:

Action	Interface_Group	Protocol	Source	Source_port	Destination	Destination_port	Host_Name
Search Action	Search Interface_Grou	Search Protocol	Search Source	Search Source_port	Search Destination	Search Destination_pc	Search Host_Name
Permit	Outside-IN	icmp	XXXX-XXXX-XXXX	any	any	any	XXXX-XXXX-XXXX
Permit	block-list_in	ip	XXXX-XXXX-XXXX	any	any4	any	XXXX-XXXX-XXXX
Permit	block-list_in	ip	XXXX-XXXX-XXXX	any	any	any	XXXX-XXXX-XXXX
Permit	Outside-IN	icmp	XXXX-XXXX-XXXX	any	any	any	XXXX-XXXX-XXXX
Permit	block-list_in	ip	XXXX-XXXX-XXXX	any	any4	any	XXXX-XXXX-XXXX
Permit	block-list_in	ip	XXXX-XXXX-XXXX	any	any	any	XXXX-XXXX-XXXX
Permit	INSIDE access in	in	XXXX XXXX XXXX	any	any	any	XXXX XXXX XXXX

3. view your dashboard

drut.

Home

Reports

Dashboards

+

drutgateway.anbglobal.com:2019/ui/init/#/dashboard?dashboardName=FIREWALL%20RULES%20WITH%20ANY%20DESTINATION&dashb...

Bot Run Date 02/08/2023 5:51:17 PM

As On To Download

FIREWALL RULES WITH ANY DESTINATION

Total Systems

Outside-IN group625

DMZ group18

Isafe_in group36

Interface Groups With Any Destination

Outside-IN group10.56 %

DMZ group33.33 %

Isafe_in group16.67 %

Risk Parameter

Firewall Rules Outside In Group3.17 %

Firewall Rules DMZ Group16.67 %

Firewall Rules Isafe_in Group3.33 %

Overall Risk

Total 23.17% Medium

Low0.00-2

Medium20.01-6

High60.01-10

Protocols Found With Any Destination

esp5.5%

icmp12.1%

icmp62.6%

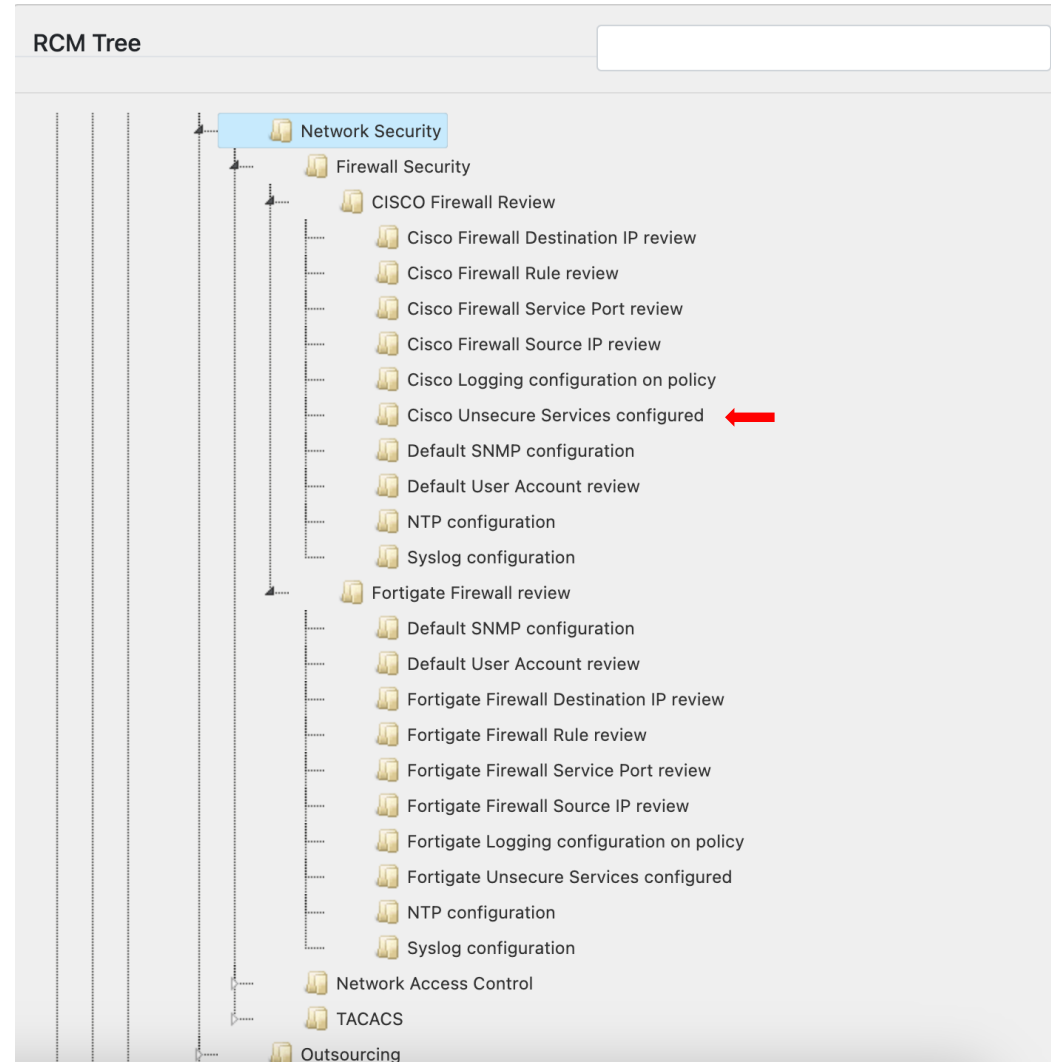
ip58.6%

ospf2.2%

tcp2.6%

udp16.5%

Another sample from drut's RCM – Risk Control Matrix



drut.

Grid

Folder

Network

Robot

Shield

Document

Checkmark

←

→

↺

🔒

drut.anbglobal.com:2019/Structure/ViewRCM

🔗

☆

🟢

f?

🐼

⚙️

⬇️

🖨️

👤

⋮

RCM

Search For

🔍

Switch to ReportBI

ANB / ANB Group / Kohinoor Bank / Technology / Network Security / Firewall Security / CISCO Firewall Review / Cisco Unsecure Services configured

Show 10 entries

Search:

RCM Tree

↕	Sub Process ↕	Activity ↕	Risk ↕	Severity ↕	Control ↕	Automatable ↕	CheckPoint ↕	Update ↕	Robo ↕
⊖	Cisco Unsecure Services configured	To ensure Firewall Services and port are not configured with unsecured services	Rules which allow or accept unsecure services or port for the systems might lead to unauthorized and unrequired access to information systems	High	Rules with unsecured Service or port should be denied or rejected and configured with approved services or port to be allow for specific required access	Yes	Verify that Firewall rules is not configure with unsecure services like telnet FTP http	Edit Activity Edit Risk	Add Collector Add Analysis

Bot Name	Condition Name	Bot Type	Bot For	Schedule Type	Last Run Time	Next Run Time	Bot Status	Results	Edit	Delete
CISCO Unsecure Services	Verify that Firewall rules is not configure with unsecure services like telnet FTP http	Analysis	Database	RunOnce	12/06/2023 16:38:13 PM	12/06/2023 16:34:00 PM	Finished	View Exceptions View ReportBI Add Risk Parameter Add Summary	Edit	🗑️

Showing 1 to 1 of 1 entries

Previous

1

Next

Download Full RCM

☒ Company

☐ Department

☐ Sub Department

Company

Download

2. find the exceptions

drut.

Grid

Documents

Network

Robot

Shield

File

Checkmark

View Report

Search For

Switch to ReportBI

Activity : To ensure Firewall Services and port are not configured with unsecured services

Annexure : List of Firewall rules is not configure with unsecure services

Base Data3145

Total Number of Rows in Base Data

Exceptions122

Number of Exceptions in Report

Deviation3%

Deviation between Total Rows and Exceptions

As On Date 06-12-2023

Summary

Preview Result

Cards & Charts

Pivot Result

Base Files

Columns: Hide

Sorting: Off

View Data: Lazy Loading

Search:

Action	Interface_Group	Protocol	Source	Source_port	Destination	Destination_port	Host_Name
Search	Search Interface	Search Protocol	Search Source	Search Sour	Search Destination	Search Destination_port	Search Host_Name
Permit	Outside-IN	tcp	any4	any	#Webex-Servers_1	HTTP	GIFRCHN01.stby
Permit	Outside-IN	tcp	any4	any	#Webex-Servers_1	www	GIFRCHN01.stby
Permit	Outside-IN	tcp	any4	any	#Webex-Servers_1	HTTP	GIFRCHN01
Permit	Outside-IN	tcp	any4	any	#Webex-Servers_1	www	GIFRCHN01
Permit	PORTAL	tcp	#PortalMMS-POOL	any	209.97.213.218	www	GIFRCHN02.stby
Permit	PORTAL	tcp	#PortalMMS-POOL	any	#PortalMMS-Servers-4	www	GIFRCHN02.stby

3% Low Risk

Download

Chart

File

Calendar

Some more firewall controls we can help with

Domain	Risk Name	Control	Checkpoint in drut
Incorrectly configured rules	Rules which allow or accept any or all destination might lead to unauthorized and unrequired access to information systems	Rules which allow or accept any or all destination might lead to unauthorized and unrequired access to information systems	Rules which allow or accept any or all destination might lead to unauthorized and unrequired access to information systems
	Rules which allow or accept any or all services or port for the systems might lead to unauthorized and unrequired access to information systems	Rules with Any or All Service or port should be denied or rejected or specified services or port should be configured to allow specific required access	Verify that Firewall rules is not configure for ANY or ALL Port services
	Rules which allow or accept any or all source systems or Users might lead to unauthorized and unrequired access to information systems	Rules with Any or All source should be denied or rejected or specified IP address or network should be configured in source address to allow specific required access	Verify that Firewall rules is not configure with ANY or ALL Source IP Address
Weak Passwords	Unauthorized and unrequired access to network device in case of default account is used	Default user account should be changed or rename and no default credential should be used for devices access	Verify that default User CISCO is not configure with CISCO password on firewall devices

Connect with Us

drut.

speed on the wire

Nirma Varma

Head Technology, Risk & Cyber Security

Nirma.varma@drut.com



Follow us on
www.drut.com
@drut.bot