מסמך הגנה

CISCO

מתגים ונתבים

נספח

תאריך: מאי 2018

משרד ראש הממשלה
מערך הסייבר הלאומי

תוכן עניינים

רקע

נספח זה הינו חלק ממסמך הגנה לציוד Cisco - מתגים ונתבים. הנספח כולל רשימת הקשחות וכן מקורות למידע נוסף.

רשימת הקשחה לנתב Cisco

מקרא - Management Plane, Control Plane, Data Plane

נושא		ערך נדרש	Router CLI	הערות
הקמת רשת ניהול נפרדת Out of Band				יש לשייך Port פיזי ל- VLAN נפרד עבור רשת ניהול OOB. הרכיב כולל גם מחבר המיועד לממשק ניהול בלבד בתצורת Out Of Band
אבטחה כללית	ניהול תצורה	Enable	Auto secure	הפעלה של מספר רב של הגדרות המקשיחות את תצורת הנתב.
DNS Lookup		Disable	No ip domain-lookup	יש לסגור שירותי ברירת מחדל שאינם דרושים לשימוש. פעולה זו מתבצעת אוטומטית כאשר מיושמת אבטחה כללית (Auto Secure) יש להבטיח ששירותי רשת שנוטרלו כברירת מחדל, ואינם דרושים, לא ייפתחו מחדש
BootP		Disable	No ip bootp server	
Service Pad		Disable	No service pad	
CDP		Disable	No cdp run Or Set cdp disable	
NTP		Disable	Ntp disable	
Keepalive		Enable	Service tcp-keepalive-in	
Aux port	מנגנוני שליטה	Disable	Transport input none	יש לאבטח את השימוש ב- aux port

	הגבלת יכולות גישה המאפשרות ביצוע פעילות שליטה בנתב	Enable	Access list (IOS)	אם אפשר לבצע פעולות שליטה ובקרה באמצעות ממשק סריאלי, נדרש שהקו כולו יהיה באזור העומד בדרישות אבטחה פיזית מתאימות. במצב זה יש לחסום את היכולת לבצע פעולות דרך ממשקי SNMP, telnet ו- http באמצעות ממשקים אחרים.
	הגבלת כתובות מורשות לביצוע פעילות שליטה במתג	Enable	Access list	שליטה ובקרה על הציוד תתבצע רק מתוך כתובות IP ספציפיות
	בקרה על מבצעי פעולות שליטה במתג	Enable	AAA authentication login (IOS)	יש להגדיר מזהים אישיים לכל אחד ממנהלני הציודה
	הצפנת התעבורה מהמנהלן אל הציוד	Enable	Crypto key (IOS) Transport input ssh (IOS)	

	רמות שליטה	יש להגדיר לפחות 2 רמות שונות של יכולת שליטה ובקרה במתג	Enable secret (IOS) Enable password (V11 or down)	
	זיהוי אישי	לכל משתמש יונפק חשבון משתמש עם זיהוי אישי חד ערכי. כל פעולת הזדהות תתבצע על בסיס זיהוי זה המשתמש יהיה אחראי על הפעולות הנעשות באמצעות חשבון זה		
	אורך סיסמא מינימלי	סיסמאות יוגדרו עפ"י מדיניות ארגונית אך לא פחות משמונה תווים למנהל מערכת, או שימוש בהגדרות NIST העדכניות	מינימום שמונה תוים	נוהלי/שרת האימות (RADIUS\TACACS PLUS)
	מורכבות סיסמא		נוהלי/Enable	נוהלי/שרת האימות (RADIUS\TACACS PLUS)
	גיל סיסמא		נוהלי	נוהלי/שרת האימות (RADIUS\TACACS PLUS)

	מגבלות על ניסיונות כניסה כושלים רצופים איפוס ניסיונות הזדהות כושלים		Set authentication ....lockout Set authentication ....Attempts	
	מניעת גניבת סיסמאות של מנהלנים מורשים		Service password-encryption	ב- CatOS לא ניתן להצפין את הסיסמאות
	הצפנת תעבורת הניהול		Crypto map	
	ניתוק חיבור לאחר פרק זמן של חוסר פעילות		Exec-timeout	
	Secure copy (SCP)	Enable	Ip scp server (IOS) Copy scp (catOS)	
	Snmp v3	Enable	Snmp-server ...v3 (IOS) Set snmp...security-model v3 (CATOS)	
	SSL	Enable	Ip http secure-server Ip http secure-client-auth	
	שרת אימות	Enable	IOS: radius-server Or Tacacs server	
מנגנוני תעבורה	נטרול ממשקים שאינם בשימוש	Enable	Shutdown (IOS)	

	מניעת תעבורה בלתי מורשת ברשת	Enable	Access list	יש להגביל את התעבורה בין ממשקים לתעבורה מורשית בלבד, יש להגביל את כתובת המקור וכתובות היעד המורשות וכן את מספרי ה- Port לתעבורת IP
	מניעת פרסום של כתובות הנתב	Enable	Interface loopback0 Source-interface	יש להגדיר Loopback עם כתובת IP שאינה ברשת החיצונית ולקשור אליו את שירותי הנתב.
	מניעת התחזויות לגורמים ברשת	Enable	Ip verify unicast revers-path Or Auto secure ... tcp-intercept	יש להשתמש באימות של Unicast reverse-path forwarding לזיהוי התחזויות IP הדבר מומלץ במיוחד לספקיות שירות, במסגרת מימוש תקן BCP38
	מניעת תקיפות המתבססות על עקיפה של מדיניות הניתוב בנתבים	Enable	No ip source route	הגדרה זו היא ברירת מחדל וכן מתבצעת אוטומטית כאשר מיושמת אבטחה כללית auto secure

	מניעת תקיפת DoS (מניעת שירות) ידועה	Enable	Ip tcp intercept or auto secure ... tcp-intercept	יש להגדיר מעקב ואישור בקשות ליצירת קשרי TCP. פעולה זו מתבצעת אוטומטית כשיש תמיכה ביכולות firewall בנתב.
	מניעת תקיפת DoS (מניעת שירות) ידועה	Enable	No ip directed-broadcast	הגדרה זו היא ברירת מחדל וכן היא מתבצעת אוטומטית כאשר מיושמת אבטחה כללית. Auto secure
	מניעת פרסום מיותר של כתובת ברשת	Enable	Ip net or no ip proxy-arp	בכדי למנוע גילוי כתובות פנימיות יש להשתמש ב- NAT (Network Address Translation) או להגביל שימוש ב- Address Resolution proxy (ARP Protocol) בממשקים חיצוניים
	הפעלת הצפנה	Enable	Crypto map	
	העברת מסרי UDP broadcast לכתובת IP ספציפית	Enable	No ip forward-protocol	

	התקנת תמיכה ויישום יכולות firewall בנתב	Enable	Ip inspect or auto secure ... Firewall	
	יישום פרמטרים לסיכול תקיפות DoS (מניעת שירות) שונות	Enable	Ip inspect parameter	כשקיימת תמיכה ביכולות firewall
	הגבלת שימוש ברוחב פס	Enable	Rate-limit	כדי להגביל את הפגיעות לתקיפות DoS שונות, ניתן להגדיר הגבלות שימוש ברוחב-פס באמצעות מנגנון ה-Committed Access Pate (CAR)
	זיהוי/מניעת תקיפות	Enable	Ip audit ... action alarm drop reset	ההתרעה נשלחת לשרת syslog ו/או לשרת ניהול מרכזי (Secure IDS Director). ניתן להוסיף תקיפות נוספות לתקיפות הבסיסיות הנבדקות, אפשרות הקיימת החל מגרסא 12.2 (11) YU או, לחלופין, גרסא 12.2 (15) T.

הגבלת יכולות ניתוב דינמי	Enable	Ip policy route-map	אם תצורת הנתבים אינה מורכבת וקיים חשש להתחזות לנתבים סמוכים כדי לשבש את פעילות הניתוב, ניתן להשתמש בניתובים סטטיים.	
מניעת השבתת המעבד	Enable	Scheduler interval	ניתן להבטיח שכל process מקבל זמן עיבוד כל פרק זמן מוגדר.	
	Enable	Scheduler allocate	אלטרנטיבית ניתן להגדיר פרק זמן מינימלי לעיבוד processes בתוך פרק זמן נתון.	
רישום ניסיונות כניסה כושלים לנתב	Enable	Login on-failure	פעולה זו מתבצעת אוטומטית כאשר מיושמת אבטחה כללית auto secure	
רישום פעולות של שולט ברמת שליטה מוגברת	Enable	AAA accounting exec		
רישום שינוי של הגדרות	Enable	AAA accounting commands	כאשר מופעל שרת אימות	
מעקב אחרי ניסיונות שליחת תעבורה בלתי מורשת	Enable	log ...	יש לרשום בלוג כל תעבורה שאינה מורשית.	

רשימת הקשחה למתג CISCO

מקרא - Management Plane, Control Plane, Data Plane

נושא		ערך נדרש	Switch CLI	הערות
הקמת רשת ניהול נפרדת Out of Band				יש לשייך Port פיזי ל- VLAN נפרד לרשת ניהול OOB. המתג כולל גם מחבר המיועד לממשק ניהול בלבד בתצורת Out Of Band
ניהול תצורה	BootP	Disable	No ip bootp server	יש לסגור שירותי ברירת מחדל שאינם דרושים לשימוש ב- IOS: שירותים אלו כוללים Tcp-small, service config, finger-mask replay, identd, udp-small-services, services UDLD ב- catos : NTP ו- UDLD
	Service Pad	Disable	No service pad	
	CDP	Disable	No cdp run Or Set cdp disable	
	NTP	Disable	Ntp disable	
	Proxy Arp	Disable	No ip proxy-arp	
מנגנוני שליטה	הגדרת כתובות המאפשרות ביצוע פעילות ניהול ושליטה במתג	Enable	Access list (IOS) Set ip permit (CatOS)	
	הגבלת כתובות לביצוע פעילות ניהול ושליטה במתג	Enable	Access list	שליטה ובקרה על הציוד תתבצע רק מכתובות IP מוגדרות

	אימות זהות מנהלני המתג	Enable	AAA authentication login (IOS) Set authentication login (catOS) AAA authentication eenable (catOS)	יש להגדיר מזהים אישיים לביצוע פעולות שליטה וניהול
	אבטחת והצפנת זהות המנהלנים	Enable	Crypto key (IOS) Transport input ssh (IOS) set crypto key (CatOS)	
	הגדרת רמות שליטה	יש להגדיר לפחות 2 רמות שונות של יכולת שליטה ובקרה במתג	Enable secret (IOS) Enable password (V11 or down) Set enable pass (CatOS)	
	זיהוי אישי	לכל מנהלן יונפק חשבון משתמש עם זיהוי אישי חד ערכי. כל פעולת הזדהות תתבצע על בסיס זיהוי זה. המשתמש יהיה אחראי על הפעולות הנעשות באמצעות חשבון זה		

	אורך סיסמא מינימלי	סיסמאות יוגדרו עפ"י מדיניות ארגונית אך לא פחות משמונה תווים למנהל מערכת, או בהתאם לתקן NIST העדכני	מינימום שמונה תווים	נוהלי/שרת האימות (RADIUS\TACACS PLUS)
	מורכבות סיסמא		Enable/נוהלי	נוהלי/שרת האימות (RADIUS\TACACS PLUS)
	גיל סיסמא		נוהלי	נוהלי/שרת האימות (RADIUS\TACACS PLUS)
	מגבלות על ניסיונות כניסה כושלים רצופים איפוס ניסיונות הזדהות כושלים		Set authentication ....lockout Set authentication ....Attempts	
	מניעת גניבת סיסמאות של מנהלנים מורשים		Service password-encryption	ב- CatOS לא ניתן להצפין את הסיסמאות
	הצפנת תעבורת הניהול		Crypto map	
	ניתוק קישור לאחר פרק זמן של חוסר פעילות		Exec-timeout	
	Secure copy (SCP)	Enable	Ip scp server (IOS) Copy scp (catOS)	
	Snmp v3	Enable	Snmp-server ...v3 (IOS) Set snmp...security-model v3 (CATOS)	
	SSL	Enable	Ip http secure-server Ip http secure-client-auth	

	שרת אימות	Enable	IOS: radius-server Or Tacacs server CatOS: Set radius server Or Set tacacs server	
מנגנוני תעבורה	נטרול ממשקים שאינם בשימוש	Enable	Shutdown (IOS) Set port disable (CatOS)	
	מניעת תעבורה בלתי מורשית ברשת	Enable	Vlan (IOS) Set VLAN (CatOS)	יש לקשר פורטים שאינם אמורים לתקשר כלל בינם לבין עצמם, ל-VLANS שונים
	מניעת תקיפת טבלת CAM במתג	Enable	Switchport port-security maximum	ב- IOS יש להגביל את מספר כתובות ה-MAC שניתן להשתמש בהן עבור הפורט
	מניעת שיבוש הגדרות vlan	Disable	No vtp mode (IOS) Set vtp mode off (CatOS)	יש לבטל שימוש ב-VTPכשאינו נחוץ
	אבטחת התחברות לרשת ע"י גורמים מזוהים בלבד	Enable	Dot1x system-auth-control (IOS) Dot1x port-control (IOS) Set dot1x system-auth-control (catOS) Set port dot1x (catOS)	קישור לרשת מחייב את יחידת הקצה בהזדהות על פי פרוטוקול 802.1x
	נדרש לביצוע אימות לגורמים המתחברים לרשת	Enable	RADIUS-SERVER HOST (IOS) Set radius server (CatOS)	אימות באמצעות 802.1x דורש שימוש בשרת רדיוס

מניעת יכולת התחברות בלתי מורשת, באמצעות מניפולציה של הגדרות trunk	Enable	IOS: Switchport trunk native vlan Switchport nonegotiate CatOS 8.3 and later: Set trunk....nonegotiate Set trunk.... None Set trunk... vlans Set trunk.... nonegotiate	יש להגביל trunks ל-vlans מוגדרים	
מניעת שיבוש טופולוגיית הרשת באמצעות פרוטוקול spanning tree	Enable	Spanning-tree portfast bpduguard (IOS) Set spantree portfast bpdu-guard (CatOS)	יש להגביל שימוש ב- STP עבור פורטים שאינם מחוברים למתג נוסף	
הגבלת ההשפעה של התקפות מניעת שירות	Enable	Storm-control broadcast level (IOS) Set spantree portfast bpdu-guard (CatOs)	יש לדכא סערות תעבורה מסוג broadcast	
	Enable	Storm-control multicast level (IOS) Storm-control unicast level (IOS)	יש לדכא סערות תעבורה מסוג unicast ו-multicast ברשתות עם חיבורים מהירים של 1Gb ומעלה	
	Enable	Set port unicast-flood disable (CatOS)	יש לדכא סערות תעבורה מסוג unicast	

	מניעת תעבורה בלתי מורשית	Enable	Access-list	אם קיימת יכולת ניתוב, יש להגביל את התעבורה בין vlans לתעבורה מורשית בלבד. יש להגביל את כתובת המקור וכתובות היעד המורשות וכן את מספרי ה- Port לתעבורת IP.
	עידון הרשאות	Enable	AAA authorization privilege....level	ב- IOS ניתן להגדיר יותר משתי רמות אבטחה, כאשר ניתן להגדיר אילו פקודות שייכות לכל רמה.
	הגבלות תעבורה	Enable	IOS Switchport port-security Or Private-vlan CATOS: Set port security Or set vlan...pvian-type	ניתן להגביל את יכולות התעבורה של ports ספציפיים ישירות או ע"י תכנון vlan פרטי.
		Enable	Vlan access-map (IOS) Set security acl map (CatOS)	ניתן להגביל תעבורה בין כתובות במתג רמה 2

	מניעת השבתת המעבד	Enable	Scheduler interval Scheduler allocate	ב- IOS ניתן להבטיח שכלprocess מקבל זמן עיבוד כל פרק זמן כפי שמוגדר. ניתן גם להגדיר פרק זמן מינימלי לעיבוד processes בתוך פרק זמן נתון.
	רישום ניסיונות כניסה כושלים למתג	Enable	AAA accounting send stop-record authentication	כשקיימת האופציה ב- IOS בלבד, יש לרשום מספר ניסיונות כניסה כושלים למתג
	מעקב אחרי פעולות ניהול המתבצעות במתג	Enable	AAA accounting exec (IOS) Set accounting exec (CatOS)	
	רישום שינוי הגדרות	Enable	AAA accounting commands (IOS) Set accounting commands (CatOS)	
	מעקב אחרי ניסיונות לביצוע תעבורה בלתי מורשית	Enable	log....	יש לרשום בלוג כל תעבורה שאינה מורשית

מקורות למידע נוסף

Cisco Best Practices

- Cisco Guide to Harden Cisco IOS Devices
- Cisco Guide to Harden Cisco IOS XR Devices
- Cisco Guide to Securing Cisco NX-OS Software Devices
- Cisco Firewall Best Practices Guide
- Protecting Your Core: Infrastructure Protection Access Control Lists

  Control Plane Policing Implementation Best Practices